Colluding Black Holes Detection in MANET

[1]Akshat Jain, [2]Shekher singh Sengar, [3]Vikas Goel
[1,2,3] Assistant Professor Panipat Institute of engg. and technology Samalkha Panipat

Abstract

A mobile ad hoc network (MANET) is an infrastructureless, dynamic network consisting of a collection of wireless mobile nodes that communicate with each other without the use of any centralized authority. MANET is an emerging research area due to its wide practical applications like in military operations, personal area networks, sensor systems and disaster situations. However, wireless MANET is particularly in danger of attacks due to its fundamental characteristics, such as wireless medium, dynamic topology, distributed cooperation, and constrained capability. Malicious intermediate nodes in wireless mobile ad hoc networks are a threat concerning security of exchanged information. Routing plays an important role in the functionality of the entire network. Routing in MANET is in danger of various attacks like worm hole, black hole, routing table overflow etc. In general, routing security in wireless MANETs appears to be a problem that is not trivial to solve. This paper presents a method to detect colluding black hole attack in AODV routing protocol.

Index Terms: MANETs, AODV, black hole, digital signature.

1. Introduction

There has been rapid growth in the use of wireless communications over the last few years, from satellite transmission to home wireless personal area networks. The primary advantage of a wireless network is the mobility i.e. ability of the wireless node to communicate with the rest of the world while being on move.

Due to absence of any fixed infrastructure and open wireless medium [1] security implementation in MANET is difficult.

In MANETs each node functions as a host as well as a router, forwarding packets for other mobile nodes in the network that may not be within direct wireless transmission range of each other. A malicious node can be a part of network and disturb the routing of packets. One of the major attacks in routing protocols is black hole attack in which a malicious node consumes all the packets destined for destination node. The malicious node launches this attack by advertising fresh route with least hop count and highest destination sequence number to the node which starts the route discovery process. The black hole node is always the first node to reply as it doesn't need to check its routing table.

In this paper, a method is proposed to detect colluding black hole nodes in Ad hoc On Demand Distance Vector (AODV) routing protocol. A Light Weight Packet (LWP) routing mechanism is devised. LWP is digitally signed up by sender. Also the concept of authentic table for neighbors is used to detect whether neighbor is authentic or not.

Section 2 discusses security services in MANETs. Section 3 gives in brief the cryptographic preface. In section 4 AODV protocol and its flaws are discussed. Section 5 discusses SAODV protocol which is an extension of AODV protocol. Section 6 presents colluding black hole attack. Section 7 gives the related work and section 8 gives the proposed solution with its algorithm and flowchart. Section 9 gives the conclusion and scope for future work.

2. Security services in MANETs

Based on their objectives, the security services [8] are classified in five categories:

Availability: Availability states that the requested services like bandwidth must be available at desired time.

Confidentiality: Confidentiality ensures that information specified should never be revealed to unauthorized entities.

Authenticity: Authenticity is a network service to determine a user's identity i.e. to legalize an authentic user.

Integrity: Integrity guarantees that information passed on between nodes has not been tempered in between the transmission.

Non-repudiation: Non-repudiation ensures that the sender cannot deny having sent the information or vice versa.

3. Cryptographic Preface [8]

Cryptography defines mathematical techniques using which data/information can be kept protected from intruders.

Cryptographic techniques are usually divided into symmetric and asymmetric cryptography techniques. In symmetric techniques, a single symmetric key is used by sender and receiver for encryption and decryption. DES and AES are examples of symmetric cryptography.

On the other hand, in asymmetric cryptography a pair of keys is used. A public key is delivered to all the parties and private key is kept private to each individual. RSA algorithm is an example of asymmetric cryptography.

Confidentiality is achieved in asymmetric cryptography when sender encrypts the information using the public key of receiver and authenticity is achieved when sender encrypts the information using the private key of its own.

Digital signature is a means of achieving both the confidentiality and authenticity. Sender encrypts the data first by receiver's public key and then by its own private key.

4. AODV [2]

A. Preliminaries and attacks

AODV is an on demand distance vector routing protocol. In on demand route is established between communicating nodes only. There is no fixed existing route as in table driven systems. Whenever a node needs to send data packets it has to initiate route discovery process.

Route discovery consists of two messages: Route Request (RREQ) and Route Reply (RREP). The source node broadcasts the RREQ messages to its neighbors which further broadcasts them to their neighbors and so on. In response to RREQ, either the destination node replies with RREP or intermediate node having route to destination replies with RREP. When intermediate node replies it is called Gratuitous Route Reply. Validity and freshness of route is decided by destination sequence number. If destination sequence number is higher than before than route is considered valid. Source selects the path for data packets transmission from which it received RREP first. Further received RREPs are discarded.

Route maintenance is done using HELLO and Route Error (RERR) packets. AODV is susceptible to following types of attacks [3]:

Black Hole: A malicious node called black hole node sends fresh enough route information to source and captures all the packets destined for destination.

Worm Hole: A collection of malicious nodes tunnels the packet in between them and disrupt the forwarding of packets.

Impersonation: In this a malicious node spoofs the other node by sending RREQ packets with a false IP address.

Flooding: Here the target is to consume bandwidth of network by flooding the network with unnecessary RREQ packets.

Denial of Service: In this attack, a malicious node disrupts the route discovery process. The malicious node is in the range of other node which sends the RREQ/RREP packets. The malicious node consumes the packets without forwarding them.

This paper concentrates on black hole attack in AODV. Next single black hole problem in AODV is summarized.

B. Single Black Hole Problem

AODV route discovery mechanism is based on RREQ/RREP messages. Source node broadcasts the RREQ message to its neighbors. Either the destination or intermediate node sends RREP. The RREP received first by source node is accepted and all further RREPs are discarded. Black hole node takes benefit of this feature of AODV and sends RREP first even without checking its routing table. In this way, a route through black hole node is setup and black hole node consumes all the forwarded packets. Since no acknowledgement is given to source node the occurrence of attack is not known to source. The concept of single black hole attack is shown in figure 1.

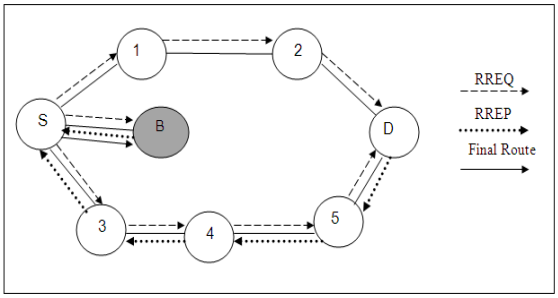

Figure 1. Single Black Hole Attack

In figure 1, B is black hole node through which final route is established. Being the black hole node, it consumes all the packets without forwarding them.

C. Solutions

In [3], RREP packet is required by intermediate node to send information about next hop. On receiving this RREP packet, source node sends a Further Request to next hop to verify that it has route to intermediate node that sends the RREP packet and it has route to destination. Further Reply is sent by next node in response to Further Request. Further Reply tells the validity of route. In [4], the solution uses the multipath routing concept. Source node checks the authenticity of node that sends RREP by finding more than one route to the destination. In [5] attack is detected using Extended Finite State Automaton (EFSA). Specification based technique and anomaly based detection is used. Also the secure routing protocol SAODV provides solution to this attack.

5. SAODV [9]

SAODV is an extension of AODV protocol. It uses the concept of double digital signature and hash chains. In SAODV double digital signature is used to protect immutable information such as destination address whereas hash chains are used to protect mutable information such as hop count.

Due to use of asymmetric cryptography the memory overhead is increased as well as processing time is increased causing delay.

Use of double signature prevents the network from black hole attack in SAODV. However, the network is susceptible to colluding black hole attack in which more than one black hole nodes work in collaboration with each other.

6. Colluding Black Hole Attack

Colluding black hole problem occurs in routing protocols when there is more than one black hole occur and they work in coordination. Colluding black hole problem is more severe than single black hole problem. Concept of colluding black hole attack is shown in figure 2 and figure 3.

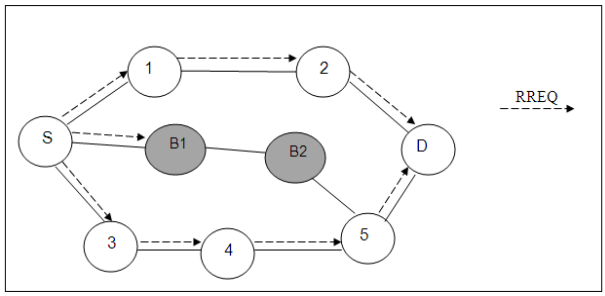

Figure 2. Broadcasting RREQ message

In figure 2 source node S broadcasts the RREQ message in the network containing black hole nodes B1 and B2. Figure also shows that black hole node B1 does not forward the RREQ message to other nodes.

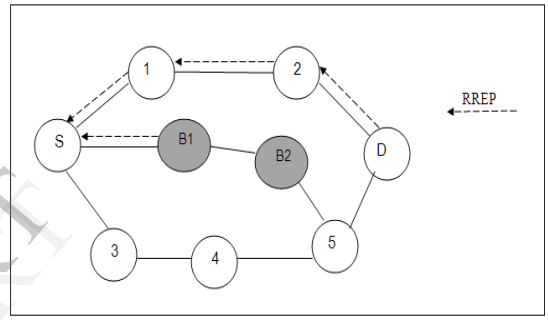

Figure 3. RREP in Colluding Black Holes

In reply to RREQ message, the B1 node sends the RREP message to source node S as shown in figure 3. Since the B1 is the first node which replies to RREQ message the colluding black hole attack occurs in the system.

Solving colluding black hole is not so easy. Neither the existing solutions to solve single black hole attack works here nor the secure routing protocol SAODV works.

7. Related Work

In [6], a Data Routing Information (DRI) table is maintained where 1 stands for 'true' and 0 for 'false'. Whenever RREP is received during the route discovery process, cross checking is done to identify whether the reply is from a reliable intermediate node.

In [7], an acknowledgement scheme is used. Some special packets called burst packets are transmitted by source to destination periodically. Destination

only needs to acknowledge for these special burst packets. Each of the ACK packets will follow a different route using a multipath routing scheme where priority is given to those nodes having a higher destination sequence number. If the number of ACK packets received is close to a threshold value and not equal to the original number of special burst packets, the source node infers that there could be some problem in the network that has caused the loss of other ACK packets. This loss can be either due to black hole nodes or due to broken links in the network. The source observes the number of ACK packets received over a period. If the trend continues to be closer to or lesser than the threshold value, it cautions the other nodes of possible intruders and initiates a black hole discovery process. When absolutely no ACK packets are received by the source, it becomes aware of the presence of adversaries in the forward path to the destination. The source now understands that no data packets have reached the intended destination and have been grabbed by one or more of the intermediate nodes.

8. Proposed Solution

In the proposed solution, the source node sends the RREQ message to the destination node. If the destination node sends the RREP itself then source node sends the data packets to destination node.

If the RREP message is sent by an intermediate node (i.e. gratuitous route reply) then in that case, one can't say whether the intermediate node is an authentic node or a black hole node.

In the proposed solution, every node maintains an authentic table of neighboring nodes along with the routing table. Authentic table contains two entries node name and 1 bit field named authentic which is set to 1 if neighboring node is authentic and 0 if neighboring node is not authentic. The format of authentic table is shown in table 1.

Table 1 Authentic Table

Neighboring Node	Authentic
-------	------
-------	------

For example, authentic table for node S in figure 3 is given below in table 2.

Table 2 Authentic Table Example

Neighboring Node	Authentic
1	1
B1	0
3	1

Before sending the data packets directly to destination node in case of gratuitous route reply, the source node checks its authentic table for authenticity of neighboring node. If the table contains an entry of 1, it means node is authentic and source node had already send data packets through that node successfully to destination already. If table entry is 0, then node is not authentic. One of the possible reasons for that can be that source node is sending the data packets through that node only for first time.

In that case, source node first sends a Light-Weight Packet (LWP) to destination node encrypted by its own private key K_{PRs} and public key of destination K_{PUd}. Since only the destination can decrypt this LWP, destination in reply sends a LWP to source encrypted by its own private key K_{PRd} and source's public key K_{PUs} through multiple paths. If source node receives this LWP from destination then source node marks neighboring node as authentic (by marking 1 in its authentic table) and sends the data packets through that neighboring node to destination. If source node doesn't receive this LWP from destination from any of the path, in that case source node knew that there is some problem. The problem can be either due to black hole nodes or due to any breaking link in between.

In this regard, source node sends a Further Request FREQ message to next to next node of neighboring node and asks for authenticity of neighboring node's next node. By checking the authentic value in its authentic table, the node replies by a Further Reply FREP message. If FREP says that node is authentic then source node sends the data packets through that neighboring node, otherwise source node marks neighboring node as black hole node and alarms the whole network about presence of colluding black hole nodes.

In this way, by the addition of a LWP the source node in the ad hoc network will be able to detect colluding black hole nodes.
The algorithm and flowchart for the proposed solution are shown in figure 4 and figure 5 respectively.

ALGORITHM

1. S sends RREP.
2. If (RREP by D) then

--- Valid Route

--- Send Data Packets and Exit.

Else [Gratuitous Route Reply]

If (authentic = 1) then [Neighboring node is authentic]

--- Valid Route

--- Send Data Packets and Exit.

Else

--- Send K_{PUd} (K_{PRs} (LWP)) to D through neighboring node.

If (K_{PUs} (K_{PRd} (LWP))) then

--- Valid Route

--- Mark 1 in authentic table.

--- Send Data Packets and Exit.

Else [LWP doesn't reach D]

--- Send FREQ to next to next node of neighboring node.

--- FREP by node from other route.

If (FREP = Yes) then

--- Authentic Node.

--- Mark 1 in authentic table.

Else

--- Colluding Black Hole nodes.

--- Alarm the network.

3. Exit.

Algorithm for proposed solution

FLOWCHART

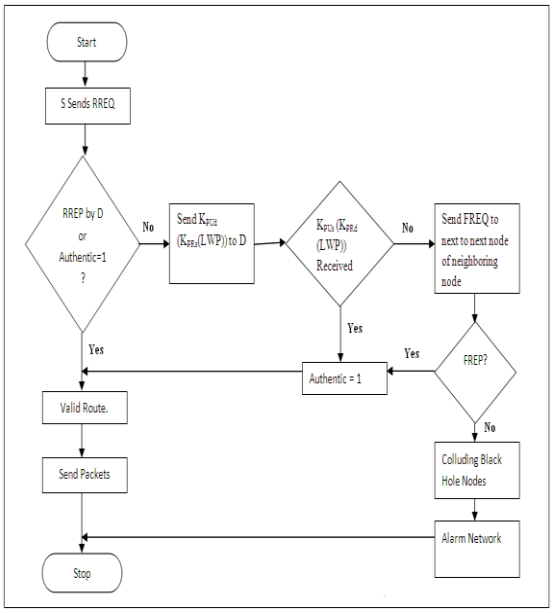

Figure a. Flowchart for proposed solution

9. Conclusion and Future Work

In this paper, the possible colluding black hole attacks that can be launched on MANET are discussed. A solution using digital signature and authentic table is also proposed. Since the proposed solution contains a LWP so not much of routing overhead increases in the network.
In short, the conclusion of work is to detect the colluding black hole nodes in the network and detach them from the network.
As a future work, our aim is to do simulation of proposed algorithm and compare it with existing solutions for optimality.

References

[1] D. P. Agrawal and Q.-A. Zeng, *Introduction to Wireless and Mobile Systems*, Brooks/Cole Publishing, Aug. 2002.

[2] C. E. Perkins and E. M. Royer, "Ad Hoc On-Demand Distance Vector Routing", *IEEE Workshop on Mobile Computing Systems and Applications* 1999, Feb. 1999, pp. 90-100.

[3] H. Deng, W. Li, and D. P. Agrawal, "Routing security in ad hoc networks," IEEE Communications Magazine, vol. 40, no. 10, pp. 70-75, Oct. 2002.

[4] M. A. Shurman, S. M. Yoo, and S. Park, "Black hole attack in wireless ad hoc networks," in ACM 42nd Southeast Conference (ACMSE'04), pp. 96-97, Apr. 2004.

[5] Y. A. Huang and W. Lee, "Attack analysis and detection for ad hoc routing protocols," in The 7th International Symposium on Recent Advances in Intrusion Detection (RAID'04), pp. 125-145, French Riviera, Sept. 2004.

[6] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, K. Nygard. "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks". Proceedings of the International Conference on Wireless Networks, June 2003.

[7] S. S. Ramaswami and S. Upadhyaya, "Smart Handling of Colluding Black Hole Attacks in MANETs and Wireless Sensor Networks using Multipath Routing". Proceedings of the 2006 IEEE Workshop on Information Assurance United States Military Academy, West Point, NY.

[8] William Stallings, *Cryptography and Network Security Principles and Practices*, Fourth Edition, Prentice Hall, Nov. 2005.

[9] Farooq Anjum and Petros Mouchtaris, *Security for Wireless Ad Hoc Networks*, John Wiley & Sons, 2007.